# Algebra liniowa dla śmiertelników

Piotr Suwara
Paweł Siedlecki

1 sierpnia 2011

# Spis treści

**1 Ciało** 2

**2 Liczby zespolone** 4

**3 Przestrzenie liniowe** 4
- 3.1 Podstawy . . . 4
- 3.2 Liniowa zależność, baza i wymiar przestrzeni . . . 6
  - 3.2.1 Przestrzenie nieskończenie wymiarowe . . . 11
- 3.3 Działania na przestrzeniach liniowych . . . 12
- 3.4 Przekształcenia liniowe . . . 13
  - 3.4.1 Rzutowania i symetrie . . . 17
- 3.5 Macierze . . . 18
  - 3.5.1 Macierze przekształceń liniowych . . . 21

**4 Przestrzenie unitarne** 22
- 4.1 Iloczyn skalarny . . . 22
- 4.2 Przestrzenie ortogonalne . . . 26

# 1 Ciało

**Definicja 1.** Zbiór $K$ z działaniami dodawania $+$ oraz mnożenia $\cdot$ (których argumentami są dwa elementy z tego zbioru, a wartościami elementy z tego zbioru) nazywamy *ciałem*, jeśli zawiera co najmniej dwa elementy oraz spełnione są tzw. aksjomaty ciała:

- łączność dodawania: $\forall_{a,b,c\in K}(a+b)+c=a+(b+c)$,
- istnienie elementu neutralnego dodawania (zera): $\exists_{0\in K}\forall_{a\in K}a+0=a$,
- istnienie elementu przeciwnego: $\forall_{a\in K}\exists_{b\in K}a+b=0$,
- przemienność dodawania: $\forall_{a,b\in K}a+b=b+a$,
- łączność mnożenia: $\forall_{a,b,c\in K}(a\cdot b)\cdot c=a\cdot(b\cdot c)$,
- istnienie elementu neutralnego mnożenia (jedynki): $\exists_{1\in K}\forall_{a\in K}a\cdot 1=a$,
- przemienność mnożenia: $\forall_{a,b\in K}a\cdot b=b\cdot a$,

- rozdzielność mnożenia względem dodawania: $\forall_{a,b,c\in K} a \cdot (b+c) = a\cdot b + a\cdot c$,
- istnienie elementu odwrotnego (dla każdego niezerowego elementu): $\forall_{a\in K\setminus\{0\}} \exists_{b\in K} a\cdot b = 1$.

Ciałami są na przykład: zbiór liczb rzeczywistych $\mathbb{R}$ (z dobrze znanymi działaniami), zbiór liczb wymiernych $\mathbb{Q}$, zbiór liczb zespolonych $\mathbb{C}$.

Ciało oprócz powyższych ma też inne często wykorzystywane własności, które wynikają wprost z aksjomatów. Poniżej podajemy przykłady takich własności. Formalne dowodzenie takich oczywistych faktów nie jest bynajmniej naszym celem, ale może być dobrym ćwiczeniem na zapoznanie się z definicją ciała – zwłaszcza, że będziemy korzystać nie tylko ze wspomnianych już ciał.

**Twierdzenie 1.** *W ciele występuje tylko jeden element neutralny dodawania (0), tylko jeden element neutralny mnożenia (1).*

*Dowód.* Załóżmy, że $0_1$ oraz $0_2$ są elementami neutralnymi dodawania. Wtedy $0_1 = 0_1 + 0_2 = 0_2$.

Zupełnie identycznie pokazuje się, że istnieje tylko jeden element neutralny mnożenia. □

**Twierdzenie 2.**

- $0 \cdot a = 0$ *dla dowolnego* $a \in K$.
- $0 \neq 1$.
- *Dla dowolnego* $a \in K$ *element do niego przeciwny nie tylko istnieje, ale jest wyznaczony jednoznacznie; oznaczmy go* $-a$.
- *Dla dowolnego* $a \in K \setminus \{0\}$ *element do niego odwrotny nie tylko istnieje, ale jest wyznaczony jednoznacznie; oznaczmy go* $a^{-1}$ *albo* $\frac{1}{a}$.

*Dowód.* Dowód pozostawiamy jako ćwiczenie. □

**Definicja 2.** $\mathbb{Z}_p$ oznacza zbiór $\{0, 1, \ldots, p-1\}$ z działaniami dodawania i mnożenia zdefiniowanymi tak, jak dla liczb całkowitych, ale modulo liczba pierwsza $p$.

Przykładowo, $\mathbb{Z}_5$ to zbiór $\{0, 1, 2, 3, 4\}$, w którym $1+2 = 3$, $2+4 = 6 \pmod 5 = 1$, $1 \cdot 4 = 4$, $3 \cdot 4 = 12 \pmod 5 = 2$.

**Twierdzenie 3.** *Dla dowolnej liczby pierwszej* $p$ *zbiór* $\mathbb{Z}_p$ *z tak określonymi działaniami jest ciałem.*

*Dowód.* Większość własności ciała możecie sami sprawdzić. Nieoczywiste pozostaje tylko, czy dla każdego niezerowego elementu istnieje element odwrotny; jest to znane twierdzenie teorii liczb i nie będziemy go tutaj udowadniać. □

Bardzo ważnym ciałem jest $\mathbb{Z}_2$. Jest to zbiór $\{0,1\}$ z działaniami takimi, że $0+0=0, 0+1=1+0=1, 1+1=0, 0\cdot 0=0, 0\cdot 1=1\cdot 0=0, 1\cdot 1=1$. Można na te działania patrzeć także jako na działania logiczne na wartościach logicznych: 0 – fałsz, 1 – prawda, + – alternatywa rozłączna (tzw. *albo*), $\cdot$ – koniunkcja (tzw. *i*).

**Definicja 3.** *Charakterystyka* ciała $K$ to najmniejsza niezerowa liczba jedynek tego ciała, jakie należy do siebie dodać, by otrzymać 0. Oznaczamy tę wartość jako $\mathrm{char}K$. Jeśli taka liczba nie istnieje, wtedy $\mathrm{char}K = 0$.

Przykładowo, charakterystyki $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ są równe 0. Z kolei $\mathrm{char}\mathbb{Z}_p = p$.

# 2 Liczby zespolone

O liczbach zespolonych możecie przeczytać na przykład na Wikipedii `http://pl.wikipedia.org/wiki/Liczby_zespolone` lub na stronie `http://www.ift.uni.wroc.pl/~cislo/algebra/wyklad5.pdf`. Z liczb zespolonych będziemy czasami korzystać, i chcielibyśmy, żebyście rozumieli: dodawanie, mnożenie, branie odwrotności, wzór de Moivre'a, sprzężenie, moduł i orientowali się, jak te definicje interpretować geometrycznie na płaszczyźnie.

# 3 Przestrzenie liniowe

## 3.1 Podstawy

**Definicja 4.** *Przestrzenią liniową* (lub *wektorową*) nad ciałem $K$ nazywamy zbiór $V$ z działaniami dodawania wektorów, które dowolnej parze elementów z $V$ (*wektorów*) przyporządkowuje inny element z $V$ (wektor), oraz mnożenia wektora przez skalar, które elementowi z ciała $K$ (*skalarowi*) oraz elementowi z $V$ (wektorowi) przyporządkowuje element z $V$ (wektor); w $V$ wyróżniony jest wektor *zerowy*, oznaczany jako 0, przy czym spełnione są następujące aksjomaty (dla dowolnych $u, v, w \in V$ oraz $a, b \in K$):

- łączność dodawania wektorów: $u + (v + w) = (u + v) + w$,
- przemienność dodawania wektorów: $u + v = v + u$,

- istnienie wektora neutralnego dodawania: $v + 0 = v$,
- istnienie wektora przeciwnego: dla $v$ istnieje takie $d \in V$, że $v + d = 0$,
- rozdzielność mnożenia względem dodawania wektorów: $a \cdot (u + v) = a \cdot u + a \cdot v$,
- rozdzielność mnożenia względem dodawania skalarów: $(a + b) \cdot v = a \cdot v + b \cdot v$,
- łączność mnożenia przez skalary: $(a \cdot b) \cdot v = a \cdot (b \cdot v)$,
- 1 jest elementem neutralnym mnożenia: $v \cdot 1 = v$.

Nie należy się przerażać powyższymi aksjomatami. Wszystkie one obrazują proste własności, których żądamy od działań dodawania wektorów i ich mnożenia przez skalary.

Szczególną rolę pełnią przestrzenie $K^n$ nad ciałem $K$. Przestrzeń $K^n$ to zbiór ciągów $n$-elementowych o elementach z ciała $K$, czyli

$$K^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$$

z naturalnie określonymi działaniami dodawania i mnożenia jako dodawanie i mnożenie po współrzędnych:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

$$c \cdot (a_1, \ldots, a_n) = (c \cdot a_1, \ldots, c \cdot a_n).$$

Najbardziej znane są przestrzenie $\mathbb{R}^n$, w szczególności $\mathbb{R}^1 = \mathbb{R}$ czyli prosta rzeczywista, $\mathbb{R}^2$ czyli dobrze znana nam płaszczyzna, $\mathbb{R}^3$ czyli przestrzeń trójwymiarowa, którą postrzegamy dookoła siebie. Dodawanie wektorów w tych przestrzeniach zdefiniowaliśmy wygląda dokładnie tak, jak jest to pokazywane w szkole. Także mnożenie przez skalar, które jest po prostu jednokładnością o skali równej temu skalarowi, czyli odpowiednim rozciąganiem.

Znowu otrzymujemy kilka oczywistych własności:

**Twierdzenie 4.**
- *Dla każdego wektora $v$ istnieje dokładnie jeden wektor przeciwny do niego $u$, czyli taki, że $v + u = 0$; oznaczamy go jako $-v$ i zachodzi równość $-v = (-1) \cdot v$.*
- *$0v = 0$ dla każdego wektora $v$ oraz $a0 = 0$ dla dowolnego skalara $a$.*
- *Jeśli $av = 0$, to $a = 0$ lub $v = 0$.*

*Dowód.* Pozostawiamy dociekliwemu czytelnikowi. □

**Definicja 5.** Niepusty podzbiór $W \subset V$ przestrzeni liniowej $V$ jest *podprzestrzenią liniową* przestrzeni liniowej $V$, jeśli jest zamknięty ze względu na działania dodawania oraz mnożenia przez skalar, czyli dla dowolnych $u, v \in W, a \in K$ zachodzi:

- $u + v \in W$,
- $av \in W$.

Łatwo sprawdzić, że działania dodawania i mnożenia w podprzestrzeni liniowej zachowują wszystkie swoje magiczne właściwości, wobec czego $W$ z tymi działaniami spełnia aksjomaty przestrzeni liniowej – jest przestrzenią liniową.

Prostym przykładem może być podprzestrzeń $W = \{(a, a) : a \in \mathbb{R}\}$ przestrzeni $V = R^2$. $V$ to cała płaszczyzna, $W$ to prosta na płaszczyźnie opisana równaniem $y = x$.

## 3.2 Liniowa zależność, baza i wymiar przestrzeni

**Definicja 6.** *Kombinacją liniową* układu wektorów $v_1, \ldots, v_n$ o współczynnikach $a_1, \ldots, a_n$ nazywamy wektor

$$u = a_1 v_1 + \ldots a_n v_n = \sum_{i=1}^{n} a_i v_i.$$

Zauważmy, że jeśli $u$ oraz $w$ są pewnymi kombinacjami liniowymi wektorów $v_1, \ldots, v_n$, to $u + w$ oraz $au$ dla dowolnego skalara $a$ też są kombinacjami liniowymi tych wektorów.

**Definicja 7.** Przez $U = \mathrm{lin}(v_1, \ldots, v_n)$ oznaczamy zbiór wszystkich kombinacji liniowych wektorów $v_1, \ldots, v_n$.

Jeśli wektory $v_i$ należą do przestrzeni $V$, to $U$ jest jej podprzestrzenią. Mówimy, że $U$ jest *przestrzenią rozpiętą* na wektorach $v_1, \ldots, v_n$. Mówimy, że te wektory *rozpinają* przestrzeń $V$, jeśli $U = V$. W takiej sytuacji każdy wektor z $V$ jest pewną kombinacją liniową wektorów z $U$.

*Uwaga* 1. Będziemy mówić, że układ współczynników $a_1, \ldots, a_n$ jest *niezerowy*, jeśli dla pewnego $j$ zachodzi $a_j \neq 0$.

Może się zdarzyć, że kombinacja liniowa wektorów o niezerowym układzie współczynników będzie wektorem zerowym! Na przykład dla $a_1 = 1, a_2 = -1, v_1 = v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ mamy $a_1 v_1 + a_2 v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$.

**Definicja 8.** Układ wektorów $v_1, \dots, v_n$ nazywamy *liniowo zależnym*, jeśli dla pewnego niezerowego układu współczynników $a_1, \dots, a_n$ ich kombinacja liniowa jest wektorem zerowym:

$$\sum_{i=1}^{n} a_i v_i = 0.$$

Jeśli nie istnieje taki niezerowy układ współczynników, to układ ten nazywamy *liniowo niezależnym.*

Równoważnie, układ $v_1, \dots, v_n$ jest liniowo niezależny, wtedy i tylko wtedy, gdy równość $\sum_{i=1}^{n} a_i v_i = 0$ implikuje $a_1 = a_2 = \dots a_n$. Jest to bardzo ważny fakt i czytelnik powinien się nad nim chwilę zastanowić.

Przykładowo, układ wektorów $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ jest liniowo niezależny (dlaczego?). Z kolei układ wektorów $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$ jest liniowo zależny (znajdź współczynniki!).

Jest jeszcze jeden ważny sposób patrzenia na liniową zależność wektorów.

**Stwierdzenie 1.** Układ $v_1, \dots, v_n$ jest liniowo zależny wtedy i tylko wtedy, gdy jeden z tych wektorów da się otrzymać za pomocą pewnej kombinacji liniowej innych.

*Dowód.* Załóżmy, że układ ten jest liniowo zależny. Wtedy $\sum_{i=1}^{n} a_i v_i = 0$ dla niezerowego układu współczynników. Przyjmijmy bez utraty ogólności, że $a_1 \neq 0$. Wtedy

$$v_1 = \sum_{i=2}^{n} -\frac{a_i}{a_1} v_i,$$

co kończy dowód implikacji w jedną stronę. Dowód w drugą stronę pozostawiamy jako ćwiczenie. □

W powyższym dowodzie pokazaliśmy, że $v_1 \in \mathrm{lin}(v_2, \dots, v_n)$. Idąc tą drogą, otrzymujemy

**Wniosek 1.** Układ wektorów jest liniowo zależny wtedy i tylko wtedy, gdy jeden z nich należy do przestrzeni rozpiętej na wszystkich innych.

Podamy kilka przydatnych faktów.

**Stwierdzenie 2.** Dany jest układ wektorów $v_1, \ldots, v_n$. Jeśli zastąpimy $v_1$ pewną kombinacją liniową o współczynnikach $a_1, \ldots, a_n$ taką, że $a_1 \neq 0$, to przestrzeń $U$ rozpięta przez otrzymany układ wektorów będzie identyczna z przestrzenią $W$ rozpiętą przez początkowy układ wektorów.

*Dowód.* Niech $v_1' = \sum_{i=1}^{n} a_i v_i$. Wtedy jeśli $W \ni v = \sum_{i=1}^{n} b_i v_i$, to $v = \frac{b_1}{a_1} v_1' + \sum_{i=2}^{n} (b_i - \frac{b_1}{a_1} a_i) v_i \in U$. Analogicznie dowodzimy $v \in U \implies v \in W$. □

Sytuacja jest identyczna, jeśli: zmienimy kolejność wektorów, pomnożymy pewien wektor przez niezerową stałą, dodamy jeden z wektorów do drugiego.

**Stwierdzenie 3.** Dany jest liniowo niezależny układ wektorów $v_1, \ldots, v_n$. Jeśli zastąpimy $v_1$ pewną kombinacją liniową o współczynnikach $a_1, \ldots, a_n$ taką, że $a_1 \neq 0$, to otrzymany układ wektorów będzie liniowo niezależny.

*Dowód.* Układ $v_2, \ldots, v_n$ jest liniowo niezależny. Gdybyśmy po dodaniu do tego układu wektora $v_1' = \sum_{i=1}^{n} a_i v_i$ otrzymali układ liniowo niezależny, to oznaczałoby to, że $v_1'$ jest kombinacją liniową $v_2, \ldots, v_n$, czyli $v_1' = \sum_{i=2} b_i v_i$, co daje nam $a_1 v_1 + \sum_{i=2}^{n} a_i v_i = \sum_{i=2}^{n} v_i$, czyli $a_1 v_1 + \sum_{i=2}^{n} (a_i - b_i) v_i = 0$. Ale początkowy układ wektorów był liniowo niezależny, czyli $a_1 = a_2 - b_2 = \ldots = a_n - b_n = 0$, co jest sprzeczne z założeniem $a_1 \neq 0$. □

Sytuacja jest identyczna, jeśli: zmienimy kolejność wektorów, pomnożymy pewien wektor przez niezerową stałą, dodamy jeden z wektorów do drugiego.

Zauważmy, że jeśli $V = \text{lin}(v_1, \ldots, v_m)$, to możemy wybrać najdłuższy taki układ wektorów $v_{j_1}, \ldots, v_{j_n}$ taki, że jest on liniowo niezależny. Okazuje się, że rozpinają one przestrzeń $V$! Dlaczego? Po pierwsze każdy inny wektor $v_i$ można otrzymać jako kombinację liniową tych wektorów, gdyż gdyby było inaczej, moglibyśmy wektor $v_i$ dołączyć do tego układu i otrzymać jeszcze dłuższy układ. Jeśli zaś całą przestrzeń $V$ da się otrzymać za pomocą wektorów $v_1, \ldots, v_n$, a każdy z tych wektorów da się otrzymać za pomocą $v_{j_1}, \ldots, v_{j_n}$. Zastanówcie się nad tym chwilę, gdyż jest to bardzo ważny wniosek. Możemy ten fakt poszerzyć:

**Twierdzenie 5.** *Skończenie generowana przestrzeń $V = \text{lin}(v_1, \ldots, v_m)$ (taka, która jest rozpinana przez skończenie wiele wektorów) posiada* bazę, *czyli taki układ liniowo niezależnych wektorów $v_{i_1}, \ldots, v_{i_n}$, które ją rozpinają. Bazę tę można wybrać spośród wektorów rozpinających tę przestrzeń.*

*Każda baza przestrzeni $V$ jest równoliczna.*

*Dowód.* Pierwszą część twierdzenia już udowodniliśmy.

Załóżmy, że $v_1, \dots, v_n$ oraz $u_1, \dots, u_k$ są bazami $V$ oraz $k < n$.

Układ $v_2, \dots, v_n$ jest liniowo niezależny oraz nie rozpina $V$, gdyż nie da się za jego pomocą otrzymać $v_1$ (konsekwencja liniowej niezależności $v_1, \dots, v_n$). Wobec tego istnieje takie $u_{i_1}$, które nie jest kombinacją liniową $v_2, \dots, v_n$ (gdyby każde $u_i$ dało się otrzymać, to dałoby się otrzymać całą przestrzeń, bo $u_1, \dots, u_n$ rozpinają tę przestrzeń). Zamieniamy więc wektor $v_1$ na $u_{i_1}$. Otrzymujemy układ $u_{i_1}, v_2, \dots, v_n$, który jest liniowo niezależny.

Znowu, zabierzmy z tego układu $v_2$. Otrzymamy układ $u_{i_1}, v_3, \dots, v_n$, który nie rozpina $V$. Wobec tego istnieje taki $u_{i_2}$, który nie jest kombinacją liniową tych wektorów. Dodajemy go do układu i otrzymujemy liniowo niezależny układ $u_{i_1}, u_{i_2}, v_3, \dots, v_n$.

Powtarzamy tę operację, aż otrzymamy liniowo niezależny układ $u_{i_1}, \dots, u_{i_n}$. Ale ponieważ $k > n$, to na pewno któreś $u$ się powtarzają: $u_{i_a} = u_{i_b}$ dla pewnych $a \neq b$. A to oczywiście znaczy, że ten układ jest liniowo niezależny. Sprzeczność. □

**Definicja 9.** Liczbę elementów dowolnej bazy $V$ nazywamy *wymiarem* przestrzeni $V$ i oznaczamy $\dim V$.

Przestrzeń nazywamy *skończenie wymiarową*, jeśli posiada ona skończoną bazę.

Posiłkując się powyższym rozumowaniem, możemy udowodnić

**Twierdzenie 6** (Steinitza)**.** *Jeśli układ wektorów $u_1, \dots, u_k$ leżących w przestrzeni liniowej $V = \text{lin}(v_1, \dots, v_m)$ jest liniowo niezależny, to:*

- *$k \leqslant m$,*
- *z układu $v_1, \dots, v_m$ można wybrać taki podukład $v_{j_1}, \dots, v_{j_{m-k}}$, że*

$$\text{lin}(v_1, \dots, v_m) = \text{lin}(u_1, \dots, u_k, v_{j_1}, \dots, v_{j_{m-k}}).$$

*W rzeczywistości w drugim punkcie pokażemy mocniejszy fakt: każdy układ liniowo niezależny $u_1, \dots, u_k$ w przestrzeni $V$ o wymiarze $n$ można dopełnić do bazy $u_1, \dots, u_k, v_{j_1}, \dots, v_{j_{n-k}}$.*

*Dowód.* Oznaczmy $\dim V = n$. Oczywiście $n \leqslant m$, gdyż bazę przestrzeni $V$ można wybrać z wektorów $v_1, \dots, v_m$.

Do układu $u_1, \dots, u_k$ rozpinającego pewną przestrzeń $U_k$ dodajmy pewien wektor $v_{j_1} \notin U_k$. Otrzymamy liniowo niezależny układ $u_1, \dots, u_k, v_{j_1}$ rozpinający pewną przestrzeń $U_{k+1}$. Znowu dodajmy wektor $v_{j_2}$ taki, który nie należy do $U_{k+1}$. Postępujmy tak do chwili, gdy otrzymamy układ $u_1, \dots, u_k, v_{j_1}, \dots, v_{j_s}$ rozpinający przestrzeń $U_{k+s}$ taką, że dla dowolnego $i$ zachodzi $v_i \in U_{k+s}$. Z jednej strony oczywiście

$U_{k+s} \subset V$, a z drugiej strony skoro $v_1, \ldots, v_n$ rozpinają $V$ i należą do $U_{k+s}$, to na pewno też $V \subset U_{k+s}$, czyli ostatecznie $V = U_{k+s}$, czyli otrzymany układ jest bazą $V$. Wobec tego $k + s$ liniowo niezależnych wektorów rozpina $n$-wymiarową przestrzeń, czyli $k + s = n$, ale $s \geqslant 0$, czyli $k \leqslant n \leqslant m$, co kończy dowód.

□

Z powyższych rozważań płyną bardzo ważne wnioski.

**Twierdzenie 7.** *Jeśli* $\dim V = n$ *oraz układ wektorów* $v_1, \ldots, v_k$ *w przestrzeni* $V$ *jest liniowo niezależny, to* $k \leqslant n$. *Jeśli* $k = n$, *to* $v_1, \ldots, v_k$ *jest bazą* $V$.

*Dowód.* Czytelnik wykorzysta poprzednie twierdzenie. □

**Wniosek 2.** Następujące warunki są równoważne:

- układ $v_1, \ldots, v_k$ jest bazą przestrzeni $V$,
- układ $v_1, \ldots, v_k$ jest największym liniowo niezależnym układem wektorów w $V$,
- układ $v_1, \ldots, v_k$ jest najmniejszym układem wektorów rozpinającym $V$.

*Dowód.* Równoważność pierwszych dwóch punktów wynika z poprzedniego twierdzenia.

Równoważność pierwszego i trzeciego punktu wynika z tego, że z każdego układu rozpinającego $V$ można wybrać bazę o liczbie wektorów równej $n = \dim V$. Wobec tego żaden układ wektorów o liczbie mniejszej niż $n$ nie może rozpinać $V$. Czyli każda baza jest najmniejszym układem układem wektorów rozpinającym $V$.

Gdyby zaś układ był najmniejszym rozpinającym $V$ i nie był bazą, to można by było z niego wybrać mniejszą od niego bazę, która byłaby mniejszym układem rozpinającym $V$.

Co kończy dowód. □

Następny wniosek mówi, że jeśli przestrzeń "siedzącą" w $V$ ma wymiar równy wymiarowi $V$, to "wypełnia" całą przestrzeń $V$.

**Wniosek 3.** Jeśli $U \subseteq V$ oraz $\dim U = \dim V$, to $U = V$.

*Dowód.* Weźmy dowolną bazę $U$, ma ona $n$ elementów. Jest to układ liniowo niezależnych wektorów z $V$ i jest ich tyle, ile wynosi $\dim V$, czyli z ostatniego twierdzenia wynika, że są bazą $V$. Wobec tego baza $U$ rozpina $V$, czyli $V \subseteq U$ i z zawierania w drugą stronę otrzymujemy $U = V$. □

**Twierdzenie 8.** *Jeśli $v_1, \dots, v_n$ jest bazą przestrzeni $V$, to dowolny wektor $v$ można w jednoznaczny sposób przedstawić jako kombinację liniową wektorów bazowych: $v = \sum_{i=1}^n a_i v_i$.*

*Dowód.* Oczywiście baza rozpina przestrzeń, czyli $v$ da się zapisać jako kombinacja liniowa wektorów bazowych: $v = \sum_{i=1}^n a_i v_i$ dla pewnych współczynników $a_1, \dots, a_n$. Pozostaje udowodnić jednoznaczność takiego zapisu. Mianowicie niech $v = \sum_{i=1}^n b_i v_i$. Wtedy otrzymujemy $\sum_{i=1}^n (a_i - b_i) v_i = 0$, ale z liniowej niezależności wektorów bazowych wynika $a_i - b_i = 0$, czyli $a_i = b_i$. Co kończy dowód. $\square$

Powyższy fakt pokazuje, że ustalając pewną bazę $B$ wektorów w $n$-wymiarowej przestrzeni $V$ nad ciałem $K$ możemy każdemu wektorowi z tej przestrzeni przypisać wektor z przestrzeni $K^n$, odpowiadający współczynnikom w odpowiedniej kombinacji liniowej. Zapisujemy to:

$$[v]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Zauważmy, że mnożąc $v$ przez skalar $a$ otrzymamy:

$$[av]_B = a[v]_B = \begin{pmatrix} a \cdot a_1 \\ a \cdot a_2 \\ \vdots \\ a \cdot a_n \end{pmatrix},$$

zaś dodając $v$ do $u$:

$$[v]_B + [u]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}.$$

### 3.2.1 Przestrzenie nieskończenie wymiarowe

Interesować nas będą przede wszystkim przestrzenie skończenie wymiarowe i część podanych przez nas twierdzeń dotyczy tylko przestrzeni skończenie wymiarowych. Powyższe rozważania pokazują, że wszystkie przestrzenie $n$-wymiarowe nad ciałem $K$ są do siebie bardzo podobne; później pokażemy, że jest to słuszna intuicja.

W rzeczywistości, gdybyśmy rozważali przestrzenie skończenie wymiarowe, wystarczyłoby definiować i dowodzić wszystko w przestrzeniach $K^n$. Jednak nie chcemy porzucać przestrzeni nieskończenie wymiarowych. Prostym przykładem przestrzeni liniowej nieskończenie wymiarowej jest przestrzeń wszystkich funkcji o argumentach i wartościach rzeczywistych ($f : \mathbb{R} \to \mathbb{R}$) nad ciałem liczb rzeczywistych. Dodawanie i mnożenie przez skalar jest naturalnie zdefiniowane: sumą funkcji $f$ i $g$ jest taka funkcja $h = f + g$, że $h(x) = (f + g)(x) = f(x) + g(x)$. Podobnie $f$ po pomnożeniu przez liczbę rzeczywistą $a$ daje taką funkcję $h = a \cdot f$, że $h(x) = (a \cdot f)(x) = a \cdot f(x)$.

## 3.3 Działania na przestrzeniach liniowych

**Definicja 10.** Jeśli mamy podprzestrzenie $U, W \subseteq V$, to *sumą* przestrzeni $U$ i $W$ nazwiemy zbiór $U + W = \{u + w : u \in U, w \in W\}$.

Można łatwo sprawdzić, że $U + W$ też jest podprzestrzenią $V$.

**Definicja 11.** Jeśli mamy podprzestrzenie $U, W \subseteq V$, to *iloczynem* przestrzeni $U$ i $W$ nazwiemy przestrzeń $U \cap W = \{v : v \in U, v \in W\}$.

Jako ćwiczenie pozostawiamy sprawdzenie, że $U \cap W$ jest podprzestrzenią $V$.

**Definicja 12.** Jeśli mamy podprzestrzenie $U, W \subseteq V$, to ich sumę $S = U + W$ nazywamy *prostą*, jeśli każdy element $s \in S$ można jednoznacznie przedstawić jako $s = u + w$ dla pewnych $u \in U, w \in W$. Taką sumę oznaczamy jako $S = U \oplus W$.

**Stwierdzenie 4.** Dla podprzestrzeni $U, W \subseteq V$ ich suma $U + W$ jest prosta wtedy i tylko wtedy, gdy $U \cap W = \{0\}$ (mówimy w takiej sytuacji, że przecięcie $U$ i $W$ jest *trywialne*).

*Dowód.* Zauważmy, że $U + W$ nie jest prosta wtedy i tylko wtedy, gdy istnieją dwie różne pary $(u_1, w_1)$, $(u_2, w_2)$, $u_1, u_2 \in U, w_1, w_2 \in W$ takie, że $u_1 + w_1 = s = u_2 + w_2$. Ale takie pary istnieją wtedy i tylko wtedy, gdy $v = u_1 - u_2 = w_2 - w_1$, ale wtedy $v = u_1 - u_2 \in U$ oraz $v = w_2 - w_1 \in W$, czyli $v \in U \cap W$. Czyli jeśli takie pary istnieją, to $U \cap W \ni v \neq 0$ (bo $u_1 \neq u_2$ lub $w_1 \neq w_2$), czyli $U \cap W$ niejest trywialne. Z kolei jeśli $U \cap W$ nie jest trywialne, to biorąc wektor $0 \neq x \in U \cap W$ oraz $u_1 = x, w_2 = x, u_2 = w_1 = 0$ otrzymujemy odpowiednią parę. Wobec tego istnienie takich par jest równoważne z nietrywialnością przecięcia $U \cap W$, co kończy dowód. $\square$

**Definicja 13.** *Podprzestrzenią dopełniającą* do podprzestrzeni $U \subseteq V$ nazywamy dowolną podprzestrzeń $W \subseteq V$ taką, że $U \oplus W = V$.

**Stwierdzenie 5.** Podprzestrzeń $W \subseteq V$ jest dopełniająca do podprzestrzeni $U \subseteq V$ wtedy i tylko wtedy, gdy $U + W = V$ oraz $U \cap W = \{0\}$.

*Dowód.* Wynika wprost z poprzedniego stwierdzenia oraz oczywistego wymogu, by suma $U + W$ wypełniała całą przestrzeń $V$. □

**Twierdzenie 9.** *Dla każdej podprzestrzeni $U \subseteq V$ istnieje przestrzeń dopełniająca $W \subset V$ i dla każdej takiej przestrzeni dopełniającej zachodzi* $\dim U + \dim W = \dim V$.

*Dowód.* Najpierw udowodnimy istnienie przestrzeni dopełniającej do $U$. Weźmy dowolną bazę przestrzeni $U$. Jest to oczywiście układ liniowo niezależny. Wobec tego na mocy tego, co udowodniliśmy przy okazji dowodu twierdzenia Steinitza, możemy ten układ dopełnić do bazy $V$. Niech $W$ będzie przestrzenią rozpiętą przez wektory dopełniające bazę $U$ do bazy $V$. Oczywiście $U + W$ to przestrzeń rozpięta przez wszystkie wektory bazowe bazy $V$, więc $U + W = V$. Z jednoznaczności zapisu wektora jako kombinacji wektorów bazowych wynika, że suma $U \oplus V$ jest prosta, co kończy pierwszą część dowodu.

Weźmy teraz dowolne podprzestrzenie $U, W \subseteq V$ takie, że $U \oplus W = V$. Wybierzmy bazę w $U$ (wektory $u_1, \ldots, u_k$) oraz bazę w $W$ (wektory $w_1, \ldots, w_l$). Udowodnimy, że wektory z obu tych baz razem tworzą bazę $V$. Mianowicie ponieważ $U + W = V$, oraz rozpinają one całe $U$ i $W$, to rozpinają one całą przestrzeń $V$. Są także liniowo niezależne, gdyż gdyby tak nie było, to pewna niezerowa kombinacja liniowa tych wektorów byłaby równa 0:

$$u + w = (\alpha_1 u_1 + \ldots + \alpha_k u_k) + (\beta_1 w_1 + \ldots + \beta_l w_l) = 0 = (0 + 0),$$

ale to jest sprzeczne z jednoznacznością zapisu $0 \in V$ jako sumy elementów $u + w$, $u \in U, w \in W$. Stąd baza przestrzeni $V$ ma $k + l$ elementów, czyli

$$\dim U + \dim W = k + l = \dim V.$$

□

## 3.4 Przekształcenia liniowe

**Definicja 14.** Niech $V, W$ będą przestrzeniami liniowymi nad ciałem $K$. Funkcję $\varphi : V \to W$ nazywamy *przekształceniem liniowym*, jeśli dla dowolnych $u, v \in V$ oraz dla każdego $a \in K$ zachodzi

- $\varphi(u + v) = \varphi(u) + \varphi(v)$,

- $\varphi(av) = a\varphi(v)$.

**Definicja 15** (suma, iloczyn)**.** Niech $\varphi, \psi : V \to W$ będą przekształceniami liniowymi. Wtedy ich *sumą* nazwiemy odwzorowanie $\varphi + \psi : V \to W$ takie, że

$$\forall_{v \in V} (\varphi + \psi)(v) = \varphi(v) + \psi(v),$$

zaś *iloczynem* $\varphi$ przez element $c \in K$ nazwiemy odwzorowanie $c\varphi : V \to W$ takie, że

$$\forall_{v \in V} (c\varphi)(v) = c \cdot \varphi(v).$$

Oczywiście w powyższych definicjach otrzymujemy odwzorowania będące również przekształceniami liniowymi.

**Definicja 16** (złożenie)**.** Niech $\varphi : V \to W, \psi : W \to Z$ będą przekształceniami liniowymi. Ich *złożeniem* nazwiemy odwzorowanie $\psi \circ \varphi : V \to Z$ takie, że

$$\forall_{v \in V} (\psi \circ \varphi)(v) = \psi(\varphi(v)).$$

**Definicja 17.** *Jądrem* przekształcenia liniowego $\varphi : V \to W$ nazywamy zbiór

$$\ker \varphi = \{v \in V : \varphi(v) = 0\} = \varphi^{-1}(0),$$

zaś *obrazem* nazywamy zbiór

$$\mathrm{im}\varphi = \{\varphi(v) : v \in V\} = \varphi(V).$$

**Stwierdzenie 6.** Jeśli $\varphi : V \to W$ jest przekształceniem liniowym, to $\ker \varphi$ oraz $\mathrm{im}\varphi$ są podprzestrzeniami liniowymi odpowiednio $V$ oraz $W$.

**Definicja 18.** *Rzędem* przekształcenia liniowego $\varphi$ nazywamy wymiar jego obrazu, czyli liczbę $\dim \mathrm{im}\varphi$.

**Definicja 19.** Przekształcenie liniowe $\varphi : V \to W$ jest:

- *epimorfizmem*, jeśli jest na,
- *monomorfizmem*, jeśli jest różnowartościowe,
- *izomorfizmem*, jeśli jest bijekcją (czyli epimorfizmem i monomorfizmem),
- *endomorfizmem*, jeśli $V = W$,
- *automorfizmem*, jeśli $V = W$ oraz $\varphi$ jest izomorfizmem.

**Stwierdzenie 7.** Przekształcenie liniowe $\varphi : V \to W$ jest epimorfizmem wtedy i tylko wtedy, gdy $\mathrm{im}\varphi = W$.

Przekształcenie liniowe $\varphi : V \to W$ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker\varphi = \{0\}$.

*Dowód.* Pierwsza część stwierdzenia wynika wprost z definicji.

Oczywiście $0 \in \ker\varphi$. Załóżmy teraz, że istnieje $x \neq 0$, $x \in \ker\varphi$. Wtedy $\varphi(0) = \varphi(x) = 0$, czyli wtedy $\varphi$ nie jest monomorfizmem. Wobec tego jeśli $\varphi$ jest monomorfizmem, to $\ker\varphi = \{0\}$. Z drugiej strony, jeśli $\varphi(x) = \varphi(y)$ dla $x \neq y$, to $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$, więc $0 \neq x - y \in \ker\varphi$. Wobec tego jeśli $\ker\varphi = \{0\}$, to $\varphi$ jest monomorfizmem. □

**Stwierdzenie 8.** Rząd przekształcenia liniowego $\varphi : V \to W$ jest nie większy, niż $\dim W$.

*Dowód.*

$$\mathrm{im}\varphi \subseteq W \implies \dim \mathrm{im}\varphi \leqslant \dim W.$$

□

**Twierdzenie 10.** *Przekształcenie liniowe $\varphi : V \to W$ jest jednoznacznie określone przez jego wartości w elementach tworzących bazę przestrzeni $V$, to znaczy jeśli $(v_1, \dots, v_n)$ jest bazą $V$, to zapisując $v$ w tej bazie oraz mając ustalone wartości $\varphi(v_1), \dots, \varphi(v_n)$ otrzymujemy*

$$\varphi(v) = \varphi(\alpha_1 v_1 + \ldots + \alpha_n v_n) = \alpha_1\varphi(v_1) + \ldots + \alpha_n\varphi(v_n).$$

*Dowód.* Dowód przez oczywistość: powyższa równość wynika z liniowości $v$, zaś jednoznaczność wynika wprost z jednoznaczności zapisania $v$ w bazie $(v_1, \dots, v_n)$. □

Udowodnimy teraz bardzo istotne twierdzenie dotyczące izomorfizmów:

**Twierdzenie 11.** *Przekształcenie liniowe $\varphi : V \to W$ jest izomorfizmem wtedy i tylko wtedy, gdy przeprowadza bazę przestrzeni $V$ na bazę przestrzeni $W$.*

*Dowód.* Załóżmy, że $\varphi$ jest izomorfizmem. Weźmy dowolną bazę $(v_1, \dots, v_n)$ przestrzeni $V$. Zauważmy, że skoro jest to baza, to wektory te rozpinają $V$, czyli każdy wektor $\varphi(v)$ można zapisać jako $\varphi(v) = \varphi(\alpha_1 v_1 + \ldots + \alpha_n v_n) = \alpha_1\varphi(v_1) + \ldots \alpha_n\varphi(v_n)$, czyli wektory $(w_1 = \varphi(v_1), \dots, w_n = \varphi(v_n))$ rozpinają $\mathrm{im}\varphi = W$. Z drugiej strony są liniowo niezależne, gdyż

$$0 = \alpha_1 w_1 + \ldots + \alpha_n w_n = \varphi(\alpha_1 v_1 + \ldots + \alpha_n v_n) \implies$$

$$\varphi(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0 \implies \alpha_1 v_1 + \ldots + \alpha_n v_n = 0 \implies \alpha_1 = \ldots = \alpha_n = 0$$

ostatnia implikacja jest prawdziwa, gdyż układ $(v_1, \ldots, v_n)$ jest bazą, czyli jest liniowo niezależny.

Załóżmy teraz, że $\varphi$ przeprowadza bazę $(v_1, \ldots, v_n)$ przestrzeni $V$ na bazę $(w_1 = \varphi(v_1), \ldots, w_n = \varphi(v_n))$przestrzeni $W$. Ale jeśli tak jest, to na pewno $\mathrm{im}\varphi = W$, gdyż wektory z bazy $W$ rozpinają $W$ oraz znajdują się w $\mathrm{im}\varphi$. Pozostało więc udowodnić, że $\ker\varphi = \{0\}$. Ale $v \in \ker\varphi \implies \varphi(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0 \implies \alpha_1\varphi(v_1) + \ldots + \alpha_n\varphi(v_n) = \alpha_1 w_1 + \ldots + \alpha_n w_n = 0 \implies \alpha_1 = \ldots = \alpha_n = 0 \implies v = 0$, co kończy dowód. □

Wnioskiem z powyższego twierdzenia jest:

**Twierdzenie 12.** *Przestrzenie $V$ i $W$ są izomorficzne wtedy i tylko wtedy, gdy $\dim V = \dim W$.*

*Dowód.* Udowodniliśmy już, że jeśli $V$ i $W$ są izomorficzne, to izomorfizm przekształca bazę jednej przestrzeni na bazę drugiej, czyli ich wymiary są równe. Jeśli zaś ich wymiary są równe, to na mocy poprzednich dwóch twierdzeń możemy określić przekształcenie $\varphi$ takie, że jeśli $(v_1, \ldots, v_n)$ oraz $(w_1, \ldots, w_n)$ są bazami $V$ i $W$ (są równoliczne, bo $\dim V = \dim W$), to $\varphi(v_1) = w_1$ i rzeczywiście to jest izomorfizm. □

Wiemy dzięki temu, że dwie $n$-wymiarowe przestrzenie liniowe nad tym samym ciałem $K$ są w swej istocie identyczne i w szczególności izomorficzne z $K^n$. Jest to bezpośrednio związane z jednoznacznością zapisu wektora z takiej przestrzeni w pewnej $n$-elementowej bazie tej przestrzeni.

**Definicja 20.** Obcięciem przekształcenia $\varphi : V \to W$ do podprzestrzeni $U \subseteq V$ nazywamy przekształcenie $\varphi|_U : U \to W$ takie, że $\varphi|_U(v) = \varphi(v)$.

**Stwierdzenie 9.** Jeśli $V = \ker\varphi \oplus U$, to przekształcenie $\varphi|_U : U \to W$ jest monomorfizmem.

*Dowód.* Z definicji obcięcia wynika wprost, że $\ker\varphi|_U \subseteq \ker\varphi$, ale przecież $\ker\varphi|_U \subseteq U$, więc $\{0\} \subseteq \ker\varphi|_U \subseteq \ker\varphi \cap U = \{0\}$, a stąd wynika, że $\ker\varphi|_U$ jest monomorfizmem. □

Obcinanie przekształcenia do podprzestrzeni dopełniającej do jego jądra tutaj służy temu, by "wyrzucić" z dziedziny tego przekształcenia jądro i zajmować się tylko istotnym "fragmentem" tego przekształcenia. Podobnie, gdy $\mathrm{im}\varphi \neq W$, zapewne będziemy chcieli ograniczyć przeciwdziedzinę tylko do istotnego fragmentu, czyli do $\mathrm{im}\varphi$.

**Stwierdzenie 10.** Przekształcenie $\varphi' : V \to \text{im}\varphi$ takie, że $\varphi'(v) = \varphi(v)$ jest epimorfizmem.

*Dowód.* Wystarczy zauważyć, że $\text{im}\varphi' = \text{im}\varphi$. □

Możemy użyć obu tych trików, by mając przekształcenie $\varphi : V \to W$ oraz rozkład $V = \ker\varphi \oplus U$ uzyskać przekształcenie $\varphi' : U \to \text{im}\varphi$ będące jednocześnie epimorfizmem i monomorfizmem, czyli izomorfizmem.

Korzystając z uzyskanych wiadomości, możemy udowodnić twierdzenie wskazujące podstawową zależność między jądrem przekształcenia i jego obrazem.

**Twierdzenie 13.** *Dla dowolnego przekształcenia liniowego $\varphi : V \to W$ zachodzi*

$$\dim\ker\varphi + \dim\text{im}\varphi = \dim V.$$

*Dowód.* Określmy przekształcenie $\varphi' : U \to \text{im}\varphi$ takie, że $\varphi'(v) = \varphi(v)$ oraz $U \oplus \ker\varphi = V$. Z powyższych dwóch stwierdzeń wynika, że jest ono izomorfizmem. Ale wobec tego $U$ oraz $\text{im}\varphi$ są izomorficzne, czyli $\dim U = \dim\text{im}\varphi$. Z drugiej strony $U \oplus \ker\varphi = V$, czyli $\dim\ker\varphi + \dim\text{im}\varphi = \dim\ker\varphi + \dim U = \dim V$, co kończy dowód. □

### 3.4.1 Rzutowania i symetrie

Z tego fragmentu skryptu najprawdopodobniej nie będziemy korzystać, ale umieszczamy go, by podać przykłady stosowania poznanych pojęć i twierdzeń.

**Definicja 21.** *Rzutowaniem* przestrzeni $V$ na podprzestrzeń $U \subseteq V$ wzdłuż dopełniającej do niej podprzestrzeni $W \subseteq V$ (czyli takiej, że $U \oplus W = V$) nazywamy przekształcenie $\psi : V \to V$ takie, że jeśli zapiszemy $v \in V$ jako sumę $v = u + w$ dla $u \in U, w \in W$, to zachodzi $\psi(v) = U$.

Zauważmy, że $\text{im}\psi = U$ oraz $\ker\psi = W$, więc $\text{im}\psi \oplus \ker\psi = V$, jeśli $\psi$ jest wskazanym powyżej rzutowaniem.

**Definicja 22.** *Symetrią* przestrzeni $V$ względem podprzestrzeni $U \subseteq V$ wzdłuż dopełniającej do niej podprzestrzeni $W \subseteq V$ (czyli takiej, że $U \oplus W = V$) nazywamy przekształcenie $\psi : V \to V$ takie, że jeśli zapiszemy $v \in V$ jako sumę $v = u + w$ dla $u \in U, w \in W$, to zachodzi $\psi(v) = -u + w$.

Zauważmy, że $\text{im}\psi = V$ oraz $\ker\psi = \{0\}$.

Z pojęciami rzutowania i symetrii wiąże się następujące stwierdzenie, które podaje ich alternatywne definicje:

**Twierdzenie 14.** *$\psi$ jest rzutowaniem wtedy i tylko wtedy, gdy $\psi^2 = \psi$ ($\psi^2 = \psi \circ \psi$).*

*$\psi$ jest symetrią wtedy i tylko wtedy, gdy $\psi^2 = \mathrm{Id}$, gdzie $\mathrm{Id}$ to przekształcenie identycznościowe, $\mathrm{Id}(v) = v$.*

*Dowód.* Czytelnik sam sprawdzi, że dla rzutowania $\psi$ zachodzi $\psi^2 = \psi$, oraz podobnie, że dla symetrii $\psi$ zachodzi $\psi^2 = \mathrm{Id}$.

Udowodnimy, że jeśli $\psi^2 = \psi$, to $\psi$ jest rzutowaniem. Mianowicie niech $U = \mathrm{im}\psi$. Zauważmy, że $\psi(U) = \psi(\psi(V)) = \psi^2(V) = \psi(V) = U$, czyli ponieważ $\dim \ker \psi|_U = \dim U - \dim \mathrm{im}\psi|_U = \dim U - \dim \psi|_U(U) = \dim U - \dim \psi(U) = \dim U - \dim U = 0$, to w $U$ nie istnieje element $u \neq 0$ taki, że $\psi(u) = 0$, więc $\ker \psi \cap U = \{0\}$. Wobec tego suma $\ker \psi + U$ jest prosta, ale $\dim \ker \psi \oplus U = \dim \ker \psi + \dim U = \dim \ker \psi + \dim \mathrm{im}\psi = \dim V$. Ponieważ $\ker \psi \oplus U \subseteq V$, to $\ker \psi \oplus U = V$. Teraz zapisując $v \in V$ w postaci $v = u + w$, gdzie $u \in U, w \in \ker \psi$ otrzymujemy $\psi(u + w) = \psi(u) + \psi(w) = \psi(u)$. Ale ponieważ $u \in \mathrm{im}\psi$, to istnieje $x$ takie, że $u = \psi(x)$. Czyli $\psi(u) = \psi(\psi(x)) = \psi^2(x) = \psi(x) = u$, czyli $\psi$ jest rzutowaniem na $U$ wzdłuż $\ker \psi$.

Udowodnimy, że jeśli $\psi^2 = \mathrm{Id}$, to $\psi$ jest symetrią. Mianowicie rozpatrzmy przekształcenie $\varphi = 2^{-1} \cdot (\mathrm{Id} - \psi)$ (element $2 = 1 + 1$ znajduje się w każdym ciele!). Otóż $\varphi^2 = (2^{-1} \cdot (\mathrm{Id} - \psi))^2 = 2^{-2} \cdot (\mathrm{Id}^2 - 2 \cdot \psi \circ \mathrm{Id} + \psi^2) = 2^{-2} \cdot (\mathrm{Id} - 2 \cdot \psi + \mathrm{Id}) = 2^{-1} \cdot (\mathrm{Id} - \psi) = \varphi$, czyli $\varphi$ jest rzutowaniem na pewną przestrzeń $U$ względem pewnej przestrzeni $W$. Z tego wynika, że dla $v \in V$, gdzie $v = u + w$, $u \in U, w \in W$, zachodzi $\psi(v) = \mathrm{Id}(v) - 2 \cdot \varphi(v) = v - 2 \cdot u = u + w - 2u = -u + w$, co oznacza, że $\psi$ jest symetrią wzdłuż $U$ względem $W$. □

## 3.5 Macierze

**Definicja 23.** *Macierzą $m \times n$* o wyrazach ze zbioru $V$ nazwiemy funkcję $A : \{1, 2 \ldots, m\} \times \{1, 2, \ldots n\} \to V$. Jej wartości na parach $(i, j)$ będziemy oznaczać $a_{ij}$ i nazywać *wyrazami* macierzy. Wygodnie jest traktować i zapisywać macierze jako prostokątne tabelki- wówczas naturalne okazuje się nazwanie wyrazów $a_{i1}, a_{i2}, \ldots, a_{in}$ oraz $a_{1j}, a_{2j}, \ldots, a_{mj}$ odpowiednio *i–tym wierszem* i *j–tą kolumną* macierzy A. Zbiór wszystkich macierzy $m \times n$ o wyrazach ze zbioru $V$ oznaczamy $M_{m \times n}(V)$.

**Definicja 24.** Niech $A \in M_{m \times n}(\mathbb{F})$. *Operacjami elementarnymi na wierszach* nazwiemy następujące operacje na $A$:

- Dodanie do jednego wiersza innego przemnożonego przez liczbę.
- Pomnożenie wiersza przez niezerową liczbę.
- Zamiana dwóch wierszy miejscami

Analogicznie definiujemy elementarne operacje na kolumnach.

**Definicja 25.** Mówimy, że macierz $A$ *jest w postaci schodkowej* gdy każdy wiersz zerowy znajduje się poniżej każdego wiersza niezerowego, oraz dla każdego wiersza jego pierwszy niezerowy wyraz znajduje się dalej na prawo niż pierwszy niezerowy wyraz w wierszu poprzednim. Gdy te pierwsze niezerowe wyrazy są jedynkami, mówimy że macierz jest w *postaci schodkowej zredukowanej.*

**Twierdzenie 15.** *Każdą macierz można za pomocą pierwszej i trzeciej elementarnej operacji na wierszach sprowadzić do postaci schodkowej, a potem stosując druga operację, do postaci schodkowej zredukowanej.*

*Dowód.* Prosta indukcja po liczbie wierszy. □

*Uwaga* 2. Relacja bycia połączonym ciągiem operacji elementarnych jest relacja równoważności w zbiorze macierzy ustalonego rozmiaru.

**Stwierdzenie 11.** Jeżeli $A'$ powstaje z $A$ za pomocą ciągu operacji elementarnych, to gdy $a_1, \dots a_n$ to wiersze $A$ mamy $\operatorname{lin}(a_1, \dots a_n) = \operatorname{lin}(a'_1, \dots a'_n)$.

*Dowód.* Skoro relacja bycia połączonym ciągiem operacji elementarnych jest relacją równoważności, to wystarczy udowodnić to stwierdzenie dla jednej operacji elementarnej-wystarczy przekonać się o jednej inkluzji powłok, ponieważ druga wyniknie z zamiany roli macierzy $A$ i $A'$. Mnożenie przez niezerowy skalar nie zmienia zbioru kombinacji liniowych, ponieważ wystarczy poprawić jeden współczynnik. Dla zamiany wierszy zamieniamy dwa współczynniki miejscami, a dla dodawania wierszy przemnażamy jeden współczynnik przez odpowiedni skalar i dodajemy do drugiego. □

*Uwaga* 3. Niech $a_1, \dots, a_n \in \mathbb{F}^n$ i $V = \operatorname{lin}(a_1, \dots, a_n)$. Wówczas gdy $A$ jest macierzą o wierszach $a_1, \dots, a_n$, a $A'$ macierzą schodkową otrzymaną operacjami elementarnymi z $A$. Wówczas niezerowe wiersze $a'_i$ tworza bazę $V$.

*Dowód.* Niezerowe wiersze tworzą układ liniowo niezależny, oraz rozpinają całą przestrzeń, skoro operacje elementarne nie zmieniają powłoki liniowej wierszy. □

*Uwaga* 4. Niech $A \in M_{m\times n}(\mathbb{F})$ będzie macierzą o kolumnach $k_1, \dots, k_n$, a $A'$ macierzą schodkową otrzymaną z $A$ za pomocą elementarnych operacji na wierszach. Jeżeli $k'_{j1}, k'_{j2}, \dots, k'_{jr}$ są kolumnami $A'$ zawierającymi pierwsze niezerowe wyrazy niezerowych wierszy $A'$, to $k_{j1}, k_{j2}, \dots, k_{jr}$ stanowią bazę przestrzeni rozpiętej przez kolumny $A$.

*Dowód.* Niech $a_1k_{j1}+\ldots+a_rk_{jr}=0$. Ta równość pozostaje prawdziwa niezależnie od operacji wykonywanych na wierszach, w szczególności dla macierzy $A'$, co oznacza że $a_1,\ldots,a_r$ są rozwiązaniem jednorodnego układu równań z macierzą współczynników o kolumnach $k'_{j1},k'_{j2},\ldots,k'_{jr}$– jest oczywiste że jedynie wektor zerowy stanowi rozwiązanie. Wystarczy teraz pokazać, że dla kazdego $j$ zachodzi $k_j\in\text{lin}(k_{j1},k_{j2},\ldots,k_{jr})$, czyli że istnieją takie $b_1,\ldots,b_r$, że $k_j=b_1k_{j1}+b_2k_{j2}+\ldots+b_rk_{jr}$, czyli równoważnie $k'_j=b_1k'_{j1}+b_2k'_{j2}+\ldots+b_rk'_{rk}$, co daje układ równań o macierzy rozszerzonej mającej kolumny $k_j1',k_j2',\ldots,k_jr',k'_j$, czyli niezawierający wiersza mającego same zera poza ostatnią kolumna, czyli jest niesprzeczny. □

**Definicja 26.** *Macierzą transponowaną* do $A\in M_{m\times n}(\mathbb{F})$ nazwiemy macierz $B\in M_{n\times m}(\mathbb{F})$, taką że $a_{ij=}b_{ji}$. Oznaczamy ją przez $A^T$.

**Stwierdzenie 12.** Dla dowolnej macierzy $A\in M_{m\times n}(\mathbb{F})$ wymiar powłoki linowej rozpietej przez wiersze $a_1,\ldots a_m$ jest równy wymiarowi powłoki liniowej rozpiętej przez kolumny $k_1,\ldots,k_n$.

*Dowód.* Sprowadźmy $A$ do postaci schodkowej. Wówczas na mocy poprzednich uwag niezerowe wiersze $a'_1,\ldots,a'_r$ są bazą $\text{lin}(a_1,\ldots,a_m)$, oraz gdy $k'_{j_1},\ldots,k'_{j_r}$ są kolumnami $A'$ zawierającymi wyrazy narożne (rozpoczynające schodki, czyli pierwsze niezerowe wyrazy w wierszach), kolumny $k_{j_1},\ldots,k_{j_r}$ stanowia bazę $\text{lin}(k_1,\ldots,k_n)$. □

**Definicja 27.** Maksymalną liczbę linowo niezależnych wierszy i kolumn macierzy $A$ nazywamy *rzędem* i oznaczamy przez $\text{r}A,\text{rk}A,\text{rank}A$.

**Twierdzenie 16** (Kronecker-Cappelli)**.** *Rozważmy układ $U$ $m$ równań linowych $n$ zmiennych o macierzy rozszerzonej $A_U$ i macierzy współczynników $A$. Wówczas układ jest niesprzeczny wtedy i tylko wtedy gdy* $\text{r}A=\text{r}A_U$. *Przestrzeń rozwiązań $W$ jednorodnego układu równań odpowiadającego $U$ ma wymiar $n-\text{r}$, oraz zbiór rozwiązań $U$ to $a+W$ gdzie $a$ jest dowolnym rozwiązaniem $U$.*

*Dowód.* Niech $a_1,a_2,\ldots,a_n,b$ będa kolumnami $A_U$, czyli $U$ ma rozwiązanie $\iff b\in\text{lin}(a_1,\ldots,a_n)\iff\text{lin}(a_1,\ldots,a_n)=\text{lin}(a_1,\ldots,a_n,b)\iff\dim\text{lin}(a_1,\ldots,a_n)=\dim\text{lin}(a_1,\ldots,a_n,b)\iff\text{r}A=\text{r}A_U$. Gdy macierz schodkowa otrzymana z $A$ ma $r$ niezerowych wierszy, to rozwiazanie układu ma $r$ zmiennych zależnych $n-r$ parametrów, czyli wymiar przestrzeni rozwiązań wynosi $n-r$, a gdy $a$ jest rozwiązaniem $U$, to $c$ jest rozwiązaniem $U$ tylko gdy $a-c\in W$. □

### 3.5.1 Macierze przekształceń liniowych

**Definicja 28.** Niech $f : V \to W$ będzie przekształceniem liniowym miedzy dwoma przestrzeniami linowymi i niech $A = \{a_1, \ldots, a_n\}$ i $B = \{b_1 \ldots, b_m\}$ będą bazami $V$ i $W$. *Macierzą przekształcenia* $f$ w bazach $A, B$ nazywamy $M \in M_{m\times n}(\mathbb{F})$, taką za dla każdego $j$ mamy $f(a_j) = \sum_{i=i}^{m} a_{ij} b_i$. Oznaczamy ją $M(f)_A^B$.

*Uwaga* 5. Przy ustalonych bazach dwóch przestrzeni przyporządkowanie każdemu operatorowi (przekształceniu) liniowemu jego macierzy w tych bazach zadaje izomorfizm między przestrzenią operatorów liniowych na tych przestrzeniach, a przestrzenią wszystkich macierzy odpowiedniego rozmiaru.

**Definicja 29.** *Iloczynem macierzy* $A \in M_{m\times k}(\mathbb{F})$ i $B \in M_{k\times n}(\mathbb{F})$ nazywamy macierz $C \in M_{m\times n}(\mathbb{F})$, taką że $c_{ij} = \sum_{l=1}^{k} a_{il} b_{lj}$ i oznaczamy $A \cdot B$ lub krócej $AB$.

*Uwaga* 6. Oznaczając przez $I$ macierz mającą zera wszędzie poza przekątna na której znajdują się jedynki otrzymujemy równości $IA = A = AI$.

**Stwierdzenie 13.** Stosując oznaczenia z definicji macierzy przekształcenia oznaczajac przez $c_1, \ldots, c_n$ i $d_1, \ldots, d_m$ są współrzędnymi wektorów $v$ i $f(v)$ w bazach $A$ i $B$, to zachodzi równość

$$M \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} d_1 \\ \vdots \\ d_m \end{bmatrix}.$$

*Dowód.* Wystarczy w wyrażaniu $f(v)$ rozpisać wektor $v$ na współrzędne, skorzystać z liniowości, rozpisać obrazy wektorów bazowych na współrzędne, skorzystać z definicji mnożenia macierzy i na koniec skorystać z jednoznaczności współczynników kombinacji liniowych. □

**Definicja 30.** Niech $A$ i $B$ będą bazami przestrzeni $V$. Wówczas macierz identyczności w tych bazach nazywamy *macierzą zmiany baz* od $A$ to $B$. Nie jest to nazwa przypadkowa, ponieważ na podstawie powyższego stwierdzenia mnożenie przez nią kolumnowego wektora zawierającego współrzędne pewnego wektora w bazie $A$ daje w wyniku kolumnowy wektor współrzędnych tego wektora w bazie $B$.

**Twierdzenie 17.** *Jeżeli* $V, W, Z$ *sa przestrzeniami liniowymi nad* $\mathbb{F}$ *z bazami* $A, B, C$, *oraz* $f : V \to W$ *i* $g : W \to Z$ *są operatorami linowymi, to* $M(g \circ f)_A^C = M(g)_B^C \cdot M(f)_A^B$.

*Dowód.* Niech $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$ i $C = \{c_1, \ldots, c_k\}$. Wówczas oznaczając małymi literami $a, b, c$ wyrazy wyżej wymienionych macierzy przekształceń otrzymujemy

$$f(a_j) = \sum_{t=1}^{m} a_{ij} b_t,\ \ g(b_t) = \sum_{i=1}^{k} b_{it} c_i,\ \ (g \circ f)(a_j) = \sum_{i=1}^{k} c_{ij} c_i,$$

a wówczas w wyrażeniu $(g \circ f)(a_j)$ ponownie rozpisując na współrzędne, korzystając z liniowości i powyższych równości otrzymujemy dla każdych $i, j$, że $c_{ij} = \sum_{t=1}^{m} b_{it} a_{tj}$. □

**Definicja 31.** Macierz $A \in M_{n \times n}(\mathbb{F})$ nazwiemy *odwracalną* gdy isnieje $B \in M_{n \times n}(\mathbb{F})$, taka że $AB = I$. Wówczas $B$ oznaczamy $A^{-1}$ i nazywamy *macierzą odwrotną* do $A$.

**Twierdzenie 18.** *Macierz $A \in M_{n \times n}(\mathbb{F})$ jest odwracalna, gdy endomorfizm $f$ przestrzeni $\mathbb{F}^n$ zadany warunkiem $A = M(f)_{st}^{st}$ jest izomorfizmem.*

*Dowód.* Gdy $AB = I$ to definiujemy endomorfizm $g$ warunkiem $B = M(g)_{st}^{st}$. Wówczas $M(fg)_{st}^{st} = M(f)_{st}^{st} M(g)_{st}^{st} = AB = I = M(id)_{st}^{st}$, czyli $f$ jest epimorfizmem między przestrzeniami tego samego wymiaru, czyli izomorfizmem. Na odwrót za pomocą izomorfizmu odwrotnego definiujemy macierz $B$, która dzięki analogicznemu rachunkowi okaże się macierzą odwrotna do $A$. □

*Uwaga* 7. Skoro izomorfizm odwrotny jest wyznaczony jednoznacznie, oraz izomorfizm odwrotny do odwrotnego to on sam to gdy $AB = I$ mamy także $BA = I$, oraz macierz odwrotna jest wyznaczona jednoznacznie.

# 4 Przestrzenie unitarne

## 4.1 Iloczyn skalarny

$\mathbb{F}$ oznacza albo $\mathbb{R}$, albo $\mathbb{C}$ (można podstawić dowolne z nich).

**Definicja 32.** *Iloczynem skalarnym* na przestrzeni wektorowej $V$ nad ciałem $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ (nie będziemy rozpatrywać innych ciał) nazwiemy funkcję $\langle \cdot, \cdot \rangle : \ V^2 \to V$ posiadającą następujące właściwości:

- Liniowość względem pierwszej zmiennej:

$$\forall_{u,v,w \in V, \alpha, \beta \in \mathbb{F}} \langle \alpha u + \beta v, w \rangle = \alpha \langle u, w \rangle + \beta \langle v, w \rangle.$$

- Symetria hermitowska:
$$\forall_{v,w\in V}\langle v,w\rangle=\overline{\langle w,v\rangle},$$
gdzie $\bar{\cdot}$ oznacza sprzężenie zespolone.
- Dodatnia określoność:
$$\forall_{v\in V}\langle v,v\rangle\geqslant 0,$$
przy czym równość zachodzi tylko dla $v=0$.

**Definicja 33.** Parę $(V,\langle\cdot,\cdot\rangle)$ będziemy nazywać przestrzenią unitarną w przypadku gdy $\mathbb{F}=\mathbb{C}$, a gdy $\mathbb{F}=\mathbb{R}$ będziemy stosowali zamiennie nazwę przestrzeń euklidesowa. W przypadku gdy jest jasne o jaki iloczyn skalarny chodzi będziemy pomijać drugi element pary.

**Definicja 34.** Długością lub normą wektora $v$ przestrzeni unitarnej $V$ nazwiemy funkcję $||\cdot||:\ V\to\mathbb{R}_0^+$ dana wzorem $||v||=\sqrt{\langle v,v\rangle}$.

*Uwaga* 8. Z definicji iloczynu skalarnego wynika, że $||\alpha v||=|\alpha|\cdot||v||$, oraz $||v||\geqslant 0$, przy czym równość zachodzi tlyko gdy $v=0$.

**Definicja 35.** Iloczyn skalarny w przestrzeni $\mathbb{R}^n$ definiujemy następująco:
$$\left(\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\right)=x_1y_1+\ldots+x_ny_n.$$

W przestrzeni $\mathbb{C}^n$ będzie to:
$$\left(\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\right)=x_1\bar{y}_1+\ldots+x_n\bar{y}_n.$$

Można sprawdzić, że powyższe definicje w przestrzeniach $\mathbb{F}^n$ spełniają wcześniej podane aksjomaty. W szczególności definicja długości wektora i iloczynu skalarnego wektora w przestrzeniach $\mathbb{R}^2,\mathbb{R}^3$ jest taka sama, jaką znamy ze szkoły.

**Stwierdzenie 14** (Najważniejsze własności iloczynu skalarnego)**.** Gdy $\langle\cdot,\cdot\rangle$ jest iloczynem skalarnym na $V$, to dla dowolnych $v_1,v_2,\ldots,v_n,w_1,w_2,\ldots w_m\in V$ i $x_1,x_2,\ldots,x_n,y_1,y_2,\ldots y_m\in\mathbb{F}$ mamy
$$\left\langle\sum_{i=1}^n x_iv_i,\sum_{j=1}^m y_jw_j\right\rangle=\sum_{i=1}^n\sum_{j=1}^m x_i\overline{y_j}\langle v_i,w_j\rangle.$$

Dla $v, w \in V$ zachodzą tzw. tożsamości polaryzacyjne: $4\operatorname{Re}\langle v, w\rangle = ||v+w||^2 + ||v-w||^2$, oraz $4\operatorname{Im}\langle v, w\rangle = ||v+iw||^2 - ||v-iw||^2$.
Każdy różnowartościowy operator (epimorfizm) $L: V \to W$, gdzie $W$ jest przestrzenią unitarną wyznacza pewien iloczyn skalarny na $V$ wzorem $\langle v_1, v_2\rangle_V = \langle L(v_1), L(v_2)\rangle_W$.

**Definicja 36.** Wektory $w, v \in V$ nazwiemy *ortogonalnymi* (prostopadłymi), gdy $\langle v, w\rangle = 0$ i oznaczamy to $v \perp w$. Podzbiory $V$ nazwiemy *ortogonalnymi* gdy ich elementy sa parami ortogonalne. Układ paramy ortogonalnych wektorów nazwiemy *ortogonalnym*, a gdy maja wszystkie normę równą 1, to taki układ nazwiemy *ortonormalnym.*

**Stwierdzenie 15** (Natychmiastowy wniosek z dwuliniowości)**.** Jedynym wektorem ortogonalnym do całej przestrzeni jest wektor zerowy.
Dla $X, Y \in V$ mamy $X \perp Y \Rightarrow Y \perp X,\ \operatorname{lin}(X) \perp \operatorname{lin}(Y)$.
Gdy $(v_i)_{i=1,\ldots,n}$ jest ortogonalnym układem wektorów ma miejsce równość Pitagorasa:

$$||\sum_{i=1}^{n} v_i||^2 = \sum_{i=1}^{n} ||v_i||^2.$$

**Twierdzenie 19** (Gram-Schidt, o ortogonalizacji)**.** *każda skończenie generowana podprzestrzeń przestrzeni unitarnej posiada bazę ortogonalną.*

**Twierdzenie 20** (O rzucie ortogonalnym)**.** *Niech* $U \leqslant V$ *i* $\dim U < \infty$*. Wówczas*

$$\forall_{v\in V} \exists! v' \in U v - v' \perp U,$$

*oraz jeżeli* $(e_1, \ldots, e_n)$ *jest ortonogonalną bazą* $U$ *zachodzi równość*

$$v' = \sum_{i=1}^{n} \frac{\langle v, e_i\rangle}{\langle e_i, e_i\rangle} e_i.$$

*Dowód.* Tych twierdzeń będziemy dowodzić jednocześnie przez indukcję- najpierw pokażmy pierwsze z nich pod założeniem, że istnieje baza ortonormalna, następnie posługując się właśnie udowodniona implikacją pokażemy drugie twierdzenie, aby na koniec wywnioskować z niego pełną wersję twierdzenia o rzucie ortogonalnym.
Niech $(e_1, \ldots, e_n)$ będzie ortogonalną bazą $U$. Wówczas każdy $v' \in U$ można zapisać jako $\sum\limits_{i=1}^{n} \lambda_i e_i$, oraz $v - v' \perp \operatorname{lin}(e_1, \ldots, e_n) = U \iff \forall_i v - v' \perp e_i$, ale $\langle v - v', e_i\rangle = 0 \iff \langle v, e_i\rangle - \lambda_i \langle e_i, e_i\rangle$ (korzystamy tytaj z dwuliniowości o ortogonalnosci bazy), czyli $v'$ spełnia żądane warunki wtedy i tlyko wtedy gdy jest zadany wzorem $v' = \sum\limits_{i=1}^{n} \frac{\langle v, e_i\rangle}{\langle e_i, e_i\rangle} e_i$.

W twierdzeniu o ortogonalizacji Grama-Schmidta układ złożony z jednego wektora jest ortogonalny. Przypuśćmy więc, że twierdzenie jest prawdziwe dla wszystkich przestrzeni unitarnych wymiaru mniejszego niż $n$. Weźmy teraz dowolną bazę $(v_1, \dots, v_n)$ i na mocy założenia indukcyjnego wybierzmy ortogonalną bazę $(e_1, \dots, e_{n-1})$ przestrzeni $\mathrm{lin}(v_1, \dots, v_{n-1})$. Teraz niech $v'$ będzie ortogonalnym rzutem $v_n$ na $\mathrm{lin}(v_1, \dots, v_{n-1})$-wówczas $v' \in \mathrm{lin}(v_1, \dots, v_{n-1})$, czyli $\mathrm{lin}(v_1, \dots, v_{n-1}, v_n) = \mathrm{lin}(v_1, \dots, v_{n-1}, v_n - v')$, oraz $v - n - v' \perp \mathrm{lin}(v_1, \dots, v_{n-1})$, czyli $\forall_i v - n - v' \perp e_i$, co oznacza że $(e_1, \dots, e_{n-1}, v_n - v')$ stanowi szukaną bazę ortogonalną.
Ostatecznie łącząc ostatnie dwa paragrafu otrzymujemy tezę twierdzenia o rzucie ortogonalnym. □

*Uwaga* 9. Każda skończenie wymiarowa przestrzeń unitarna posiada bazę ortonormalną i każdy układ ortonormalny (który jest oczywiście liniowo niezalzeżny) daje się uzupełnić do bazy ortonormalnej.

*Dowód.* Istnienie bazy ortonozmalnej wynika natychmiast z twierdzenia o ortogonalizacji. uzupełniając nasz układ ortonormalny do jakejkolwiek bazy możemy przeprowadzić ortogonalizację otrzymanej bazy i zauwazyć że początkowe ortonormalne wektory nie ulegną zmianie. □

**Twierdzenie 21.** *Rzutowanie ortogonalnie nie zwiększa normy wektorów, a nierówność jest ostra, gdy rzutowany wektor nie należy do podprzestrzeni na która rzutujemy.*

*Dowód.* Jeżeli rzutujemy $v$ na $U$ i $v \in U$, to jego rzutem jest on sam (spełnia wymagane warunki, a rzut jest wyznaczony jednoznacznie). W przeciwnym wypadku ma miejsce równość Pitagorasa $||v||^2 = ||v'||^2 + ||v - v'||^2$, przy czym $||v - v'||^2 \neq 0$. □

**Wniosek 4** (Cauchy-Buniakowski-Schwarz)**.** $|\langle v, w \rangle| \leqslant ||v|| \cdot ||w||$, przy czym równość zachodzi gdy $v, w$ są linowo zależne.

*Dowód.* Gdy $w = 0$ zachodzi równość. W przeciwnym wypadku rzutując $v$ na $\mathrm{lin}(w)$ na mocy poprzedniego twierdzenia i twierdzenia o rzucie ortogonalnym otrzymujemy $\frac{|\langle v, w \rangle|}{||W||} \leqslant ||v||$, oraz odpowiednie warunki opisujące przupadek równości. □

**Wniosek 5** (Bessel)**.** Gdy $(e_1, \dots, e_n) \in V$ jest ortonormalny, to $\sum\limits_{i=1}^{n} |\langle v, e_i \rangle|^2 \leqslant ||v||^2$ i równość zachodz gdy $v \in \mathrm{lin}(e_1, \dots, e_n)$.

*Dowód.* Rzutując $v$ na $\mathrm{lin}(e_1, \dots, e_n)$ otrzymujemy na podstawie równości Pitagorasa $||v'||^2 = \sum\limits_{i=1}^{n} |\langle v, e_i \rangle|^2 \leqslant ||v||^2$, czyli teza wraz z przypadkiem równości wynika z udowodnionego twierdzenia. □

## 4.2 Przestrzenie ortogonalne

**Definicja 37.** Dla dowolnego podzbioru $A \subset V$ przez $A$ *ortogonalne* lub *anihilator* rozumiemy zbiór $\{v \in V \quad v \perp A\}$. A ortogonalne oznaczamy $A^{\perp}$.

**Stwierdzenie 16** (Najwazniejsze własności anihilatora)**.** Dla dowolnych podzbiorów $A, B \subset V$ mamy

- $A^{\perp} = \bigcap_{a \in A} a^{\perp}$ i jest to podprzestrzeń $V$.
- $(A \cup B)^{\perp} = A^{\perp} \cap B^{\perp}$.
- $A \subset B \Rightarrow A^{\perp} \supset B^{\perp}$.
- $(\mathrm{lin} A)^{\perp} = A^{\perp}$.

**Definicja 38.** Mówimy, że $V$ jest *suma ortogonalną* podprzestrzeni $V_i$ gdy jest ich sumą algebraiczną i są one parami ortogonalne. Gdy zawiera ona dwa składniki to każdy z nich nazywamy *dopełnieniem ortogonalnym* drugiego.

*Uwaga* 10. Suma ortogonalna jest prosta, bo dla każdej zerowej kombinacji liniowej suma kwadratów norm składników na mocy ortogonalności i równości Pitagorasa jest 0, czyli wszystkie składniki są 0 na mocy dodatniej określoności normy.

*Uwaga* 11. Z poprzedniej uwagi wynika, że ortogonalne układy niezerowych wektorów są liniowo niezależne (Ich powłoki linowe tworzą sumę prostą, czyli w szczególności żaden nie należy do powłoki liniowej pozostałych).

**Stwierdzenie 17.** Dopełnienia ortogonalne są nawzajem swoimi anihilatorami.

*Dowód.* Jeżeli $U, W$ sumują się ortogonalnie do $V$ to mamy $W \subset U^{\perp}$, ale dla $v \in U^{\perp}$ zapisując go jako sumę dwóch prostych składników otrzymujemy $0 = \langle u, v \rangle = ||u||^2 + \langle u, w \rangle$, czyli składnik $u = 0$, czyli $v \in W$. □

**Stwierdzenie 18.** Skończenie wymiarowa podprzestrzeń posiada jednoznacznie określone dopełnienie ortogonalne–swój anihilator.

*Dowód.* Z twierdzenie o rzucie ortogonalnym wynika, że $U$ i $U^{\perp}$ sumują się algebraicznie do całej przestrzeni (rzutując dowolny wektor na $U$ dostajemy szukany rozkład). Jednoznaczność wynika z poprzedniego twierdzenia. □

**Wniosek 6.** Dla $U \leqslant V$ mamy $\dim U^{\perp} = \dim V - \dim U$.

*Dowód.* Na podstawie poprzednich trzech stwierdzeń $U$ i jej anihilator sumują się prosto do $V$, czyli pozostaje już tylko skorzystać z twierdzenia 9. □

**Stwierdzenie 19.** Jeżeli podzbiór $A \subset V$ ma skończenie wymiarową powłokę liniową, to $(A^{\perp})^{\perp} = \text{lin}A$.

*Dowód.* Na podstawie stwierdzeń 16 i 17 mamy $A^{\perp} = \text{lin}A^{\perp}$, czyli po skorzystaniu z $\left(U^{\perp}\right)^{\perp} = U$ dostajemy tezę. □

**Definicja 39.** Dysponując już pojęciem przestrzeni wzajemnie ortogonalnych możemy zdefiniować *rzut i symetrię ortogonalne* względem i na/wzdłuż podprzestrzeni sumujących się ortogonalnie. W przypadku rzutu nie jest to konflikt oznaczeń ponieważ wynik działania tego operatora, bez niespodzianki, okazuje się być rzutem ortogonalnym z twierdzenia o rzucie ortogonalnym.